Form PTO-1449 (Modified)	ATTY DOCKET NO. B-4253PCT 618967-4	U.S. SERIAL NO. 09/913,003
LIST OF PATENTS AND PUBLICATIONS STATEMENT	APPLICANT Wenbo Mao	
	FILING DATE August 8, 2001	GROUP not yet assigned

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	ISSUE DATE	NAME	CLASS	SUB-CLASS	FILING DATE or 102(e) DATE IF APPROPRIATE
ZD		4,633,036	12/86	Hellman, et al.	178	22.11	
ZD		4,405,829	09/83	Rivest, et al.	178	22.1	

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	PUBLICATION DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES/NO
ZD		0 534 420 A2	3/31/93	EP	—	—	
ZD		0 202 768 A2	11/26/86	EP	—	—	

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

ZD	✓	Berger, Richard, et al., "A Framework for the Study of Cryptograhic Protocols," *Advances in Cryptology-Proceedings of CRYPTO 85, Lecture Notes in Computer Science*, Springer-Verlag, pp. 87-103 (August 1985).
ZD	✓	Blum, Manuel, "Coin flipping by telephone: a protocol for solving impossible problems," *Proceedings of 24th IEEE Computer Conference (CompCon)*, pp. 133-137 (February 1982).
ZD	✓	Goldwasser, Shafi, "Multi-Party Computations: Past and Present," *Proceeding of the 16th Annual ACM Symposium on Principles of Distributed Computing*, pp. 1-6 (August 1997).
ZD	✓	Camenisch, Jan and Michels, Markus, "Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes," *Advances in Cryptology-EUROCRYPT 99, Lecture Notes in Computer Science*, Springer-Verlag, 1592, pp. 106-121 (1999).
ZD	✓	Liskov, Moses and Silverman, Robert D., "A Statistical Limited-Knowledge Proof for Secure RSA Keys," *5th ACM Conference on Computer and Communications Security*, IEEE P1363 Research Contributions, pp. 1-14 (1998).

20	✓	Damgard, Ivan Bjerre, "Practical and Provable Secure Release of a Secret and Exchange of Signatures," *Advances in Cryptology-Proceedings of EUROCRYPT 93, Lecture Notes in Computer Science*, Springer-Verlag, 765, pp. 200-217 (1994).
21	✓	Karanakis, E., *Primality and Cryptography*, Wiley-Teubner Series in Computer Science, John Wiley & Sons, p. 28 (1986).
22	✓	Blackburn, S.R. and Galbraith, Steven D., "Certification of Secure RSA Keys," *Technical Report CORR 90-44*, University of Waterloo Centre for Applied Cryptographic Research, pp. 1-10 (May 6, 1999).
23	✓	Boyar, Joan, et al., "Practical Zero-Knowledge Proofs: Giving Hints and Using Deficiencies," *Advances in Cryptology-Proceedings of EUROCRYPT 89, Lecture Notes in Computer Science*, Springer-Verlag, 434, pp. 155-172 (1990).
24	✓	Galil, Zvi, et al., "A Private Interactive Test of a Boolean Predicate and Minimum-Knowledge Public-Key Cryptosystems," *26th FOCS*, pp. 360-371 (1985).
25	✓	Gennaro, Rosario, et al., "An Efficient Non-Interactive Statistical Zero-Knowledge Proof System for Quasi-Safe Prime Products," *5th ACM Conference on Computer and Communications Security*, pp. 1-13 (October 1998).
26	✓	Van de Graaf, Jeroen and Peralta, Rene, "A Simple and Secure Way to Show the Validity of Your Public Key," *Advances in Cryptology-Proceedings of CRYPTO 87, Lecture Notes in Computer Science*, Springer-Verlag, 293, pp. 128-134 (1988).
27	✓	ISO/IEC 9798-3, "Information technology - Security techniques - Entity authentication mechanisms; Part 3; Entity authentication using a public key algorithm," International Organization for Standardization, Geneva, Switzerland, pp. 1-9 (1993).
28	✓	Micali, Silvio, "Fair Public-Key Cryptosystems," *Advances in Cryptology-Proceedings of CRYPTO 92, Lecture Notes in Computer Science*, Springer-Verlag, 740, pp. 113-138 (1993).
29	✓	Solovay, R. and Strassen, V., "A Fast Monte-Carlo Test for Primality," *SIAM Journal of Computing*, Vol. 6, No. 1, pp. 84-85 (March 1977).

EXAMINER	DATE CONSIDERED
Zachary Davis	3/11/05

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.